Claims

1. Method for protecting an encrypted content by means of at least one encryption key and transmitted by a diffuser to at least one multimedia unit associated to a security module, a value allowing the determination of the encryption key(s) of this content also being transmitted to the multimedia unit by said diffuser, said security module comprising means to determine the encryption key on the basis of said value, this method comprising the following steps:

- generation of a temporary encryption key (MCW),
- encryption by the temporary key (MCW) of the value allowing the determination of the encryption keys (cw) of the content;
- transmission of this encrypted value to said multimedia unit,
- encryption and transmission of at least two cryptograms comprising the temporary key (MCW) encrypted by an authorization key (G), the first cryptogram being encrypted by a first authorization key pertaining to a first security module and the second cryptogram being encrypted by a second authorization key pertaining to a group of security modules whose first security module is excluded.

2. Method according to claim 1, **characterized in that** said value allowing the determination of the encryption key(s) of the content is the encryption key itself.

3. Method according to claim 1, **characterized in that** said value allowing the determination of the encryption key(s) of the content includes at least one variable element (RN) and in that said encryption key (cw) is built from this variable element (RN).

4. Method according to claim 3, **characterized in that** said value allowing the determination of the encryption key(s) furthermore includes an additional element (CD) related to the content (CT) in addition to the variable element (RN).

5. Method according to claim 4, **characterized in that** said additional element (CD) contains the conditions to access to the transmitted content (CT).

6. Method according to claim 3, **characterized in that** said encryption key (cw) is built by means of a hash function applied at least to said variable element (RN).

7. Method according to claim 3, **characterized in that** said encryption key (cw) is built by means of an encryption function applied at least to said variable element (RN).

8. Method for protecting an encrypted content by means of at least one encryption key and transmitted by a diffuser to at least one multimedia unit associated to a security module, a value allowing the determination of the encryption key(s) of this content also being transmitted to the multimedia unit by said diffuser, said security module comprising means to determine the encryption key on the basis of said value, this method comprising the following steps:

- generation of said value allowing the determination of the encryption key(s);
- transmission of said value to the multimedia unit, allowing the deduction of the encryption key (cw) of the content,
- generation of a temporary encryption key (MCW),
- transformation, by the temporary key (MCW), of the value allowing the determination of the encryption keys of the content, this transformation giving as a result, said encryption key (cw) of the content;
- encryption and transmission of at least two cryptograms comprising the temporary key (MCW) encrypted by an authorization key (G), the first cryptogram being encrypted by a first authorization key pertaining to a first security module and the second cryptogram being encrypted by a second authorization key which pertains to a group of security modules, whose first security module is excluded.

9. Method according to claim 8, **characterized in that** said value allowing the determination of the encryption key(s) of the content includes at least one variable element (RN) **and in that** said encryption key (cw) is built from this variable element (RN).

10. Method according to claim 9, **characterized in that** said value allowing the determination of the encryption key(s) further includes an additional element (CD) in addition to the variable element (RN).

11. Method according to claim 10, **characterized in that** said additional element (CD) contains the conditions to access to the transmitted content (CT).

12. Method according to claim 8, **characterized in that** the transformation is a hash operation with key, the key being the temporary encryption key (MCW).

13. Method according to claim 8, **characterized in that** the authorization keys (G) are classified in levels, the keys of the highest level being unique and individual for one security module, the key of the lowest level being known by all the security modules and the intermediate level keys being common to a security module subset, this subset not containing all the modules.

14. Method according to claim 13, intended for the revocation of one or several security modules, **characterized in that**, as a second authorization key (G) intended for the encryption of the temporary key, the keys common to the largest possible group of security modules are used, this group not including the revoked security module(s).

15. Method according to claim 13, **characterized in that** a message is sent to the security modules, indicating the level of the authorization key (G) which must be used.